*BY ORDER OF THE*
*SECRETARY OF THE AIR FORCE*

*AIR FORCE INSTRUCTION 31-701*

*18 FEBRUARY 1994*

***Security***

***PROGRAM PROTECTION PLANNING***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

---

OPR: HQ AFMC/SPX (Mr Larry D. Huyett)

Certified by: HQ USAF/SP (Brig Gen Stephen C. Mannell)

Pages: 14

Distribution: F

---

This instruction implements AFPD 31-7, *Acquisition Security*, and Department of Defense (DoD) Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, by providing guidelines and procedures to prepare and coordinate a program protection plan. This instruction complements AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures* (formerly AFR 57-1); AFI 16-101, *International Affairs and Security Assistance Management* (formerly AFRs 75-43, 130-1, 130-2, and 200-5); AFI 31-101, *The Air Force Physical Security Program* (formerly AFRs 207-1, 207-2, 207-4, 207-5, 207-6, 207-7, 207-8, 207-21, 207-23); AFI 31-702, *Systems Security Engineering*; and AFI 31-703, *Product Security*.

***SUMMARY OF REVISIONS***

This is the initial publication of AFI 31-701.

**1. Air Force Program Protection Planning Process.** The Air Force program protection planning process meets the Air Force's needs for acquiring and fielding secure and uncompromised weapon systems. The program identifies and protects classified and sensitive information for each defense acquisition program. Apply program protection from Phase 0, through all phases of the acquisition process, to system retirement.

1.1. This instruction does *not* replace security policies in existing security programs, but rather integrates the programs into a team approach that concentrates on risk analysis. Program protection planning provides program managers, system owners, and users with an overall view of threats to the system and planned security countermeasures they can use to counter such threats.

1.2. Program protection planning provides a basis for balancing security countermeasures, security costs, and risks to the system being procured. This instruction establishes no new requirements,

except those inherent in the protection plan itself. In implementing this plan, each security area contributes a portion to the plan using formats prescribed by policy makers.

**1.3. Responsibilities:**

- The Chief of Security Police (HQ USAF/SP) 1340 Air Force Pentagon, Washington DC 20330-1340, is responsible for physical security, information security, personnel security, industrial security, system security engineering, program protection planning, and Product Security.
- DCS Command, Control, Communications & Computers (HQ USAF/SC), 1250 Air Force Pentagon, Washington DC 20330-1250, is responsible for information systems security, communications security, and compromising emanations (TEMPEST).
- Headquarters, 497th Intelligence Group, Directorate of Security and Communications (HQ 497th IG/INS), 211 Brookley Ave, Suite 200, Bolling AFB DC 20332-5108, is responsible for security of Sensitive Compartmented Information.
- The Chief of Foreign Disclosure Policy Branch, Deputy Under Secretary of the Air Force for International Affairs (SAF/IADP), 1010 Air Force Pentagon, Washington DC 20330-1010, is responsible for foreign disclosure guidance.
- DCS Plans and Operations, Technical Plans Division (HQ USAF/XOXT), 1480 Air Force Pentagon, Washington DC 20330-1480, is responsible for Operations Security (OPSEC).
- Headquarters, Air Force Office of Special Investigations (HQ AFOSI/IOC), 226 Duncan Ave, Bolling AFB DC 20332-0001, is responsible for counterintelligence support.
- Acquisition Management and Policy Division, Deputy Assistant Secretary of the Air Force for Management Policy and Programs Integration (SAF/AQXA), 1060 Air Force Pentagon, Washington DC 20330-1060, is responsible for acquisition security.

## 2. Program Protection Plan (PPP):

2.1. Preparation and implementation of a PPP for an acquisition program or system relies on risk management, not risk avoidance. You should balance the cost of protecting the system's critical information against the cost and impact of these items.

2.2. The protection plan integrates and manages system security for an acquisition program throughout its life span.

2.3. DoD Instruction 5000.2, AFPD 10-6, *Mission Needs and Operational Requirements*, and AFI 10-601 require that all Air Force acquisition programs develop a PPP. Minimally, management must complete the PPP and the appropriate Milestone Decision Authority must review at Milestone I. The PPP must be reviewed and updated at each subsequent milestone.

2.4. For acquisition programs that have already progressed beyond Milestone I and which have not yet prepared a PPP, owning or using major commands (MAJCOM) must develop and maintain a PPP to address the remainder of the system's life.

2.5. Responsibilities for the PPP:

- System program director has ultimate responsibility for the PPP, although the user commands must agree to the plan.

- System program directors designate someone to coordinate all protection planning activities, and work closely with security professionals to implement a comprehensive PPP by Milestone I. The system program director also makes sure to update the PPP at subsequent milestones. **Attachment 1** shows key exit criteria for the PPP as defined in DoD Instruction 5000.2.
- Program managers identify an office of primary responsibility for PPP development before reaching Milestone I. Operating and implementing commands work together to develop PPP.

2.6. PPP development and implementation require close coordination between the program director, key members of the program office, the user commands, and security professionals.

2.7. Establish a system security working group (SSWG) for Acquisition Category (ACAT) I or II programs (reference AFI 31-702) to serve as the coordination arm of the system program office (SPO). SPO's can create a SSWG for this purpose for ACAT III or IV programs. The SSWG should establish the basic elements of the PPP before they forward the plan for review. The SSWG should include, but not be limited to, user command representatives for the following areas:

- Program Office.
- Program Engineer.
- Program Scientist.
- Information Security.
- Industrial Security.
- Personnel Security.
- Physical Security.
- System Security Engineering.
- Foreign Disclosure Office.
- Special Security Office.
- Communications Security.
- TEMPEST.
- Information Systems Security.
- Counterintelligence.
- Operations Security.
- Special Access Program Representative (where applicable).
- Science and Technology Control.

**3. Protection Planning Process.** Program protection planning employs a step-by-step analytical process. The process will:

- Identify the essential program information, technologies, and systems (EPITS) information.
- Analyze the threats.
- Determine program vulnerabilities.
- Assess the risks to the EPITS.
- Apply countermeasures.

3.1. As the program matures, repeat the process, taking into account changes in sensitivity of essential program information, technologies, systems, and the threat. These changes can alter program vulnerabilities, and change or eliminate countermeasures.

**4. PPP Considerations.** The PPP is the single-source document to coordinate and integrate all program protection efforts.

4.1. The considerations listed in the following **4.2.** section may or may not apply to each acquisition. Tailor considerations to the specific needs of the particular program.

4.2. PPP considerations should include, but need not be limited to, the listed areas:

- System description.
- Program information.
- EPITS.
- Adversary threats.
- Vulnerabilities.
- Time-phased plan of protection
- (countermeasures).
- Protection costs.
- Time- or event-phased security classification guide.
- Technology Assessment/Control Plan (TA/CP).
- System Security Management Plan.
- Other security plans as required by the SSWG.

4.3. Evaluate the plan's security classification by considering the PPP's scope and focus. Use the work sheet in **Attachment 2** to gather information to prepare the PPP. The worksheet is not a boilerplate, "fill-in-the-blank" program protection plan. Use it when you gather data for PPP planning, development, and update.

4.4. Although you must complete a PPP for all acquisition programs, your level of effort will vary according to the type of acquisition. For instance, when you acquire commonly available items that don't need additional security, a one to two page PPP that explains security is probably all you need.

**4.5. System Description.** The system description should clearly indicate the system's capabilities and limitations. Use the Operational Requirements Document as required by AFI 10-601 to find the system capabilities and characteristics. The system description must address the following areas:

- Anticipated battlefield use.
- Strategic, operational, or tactical impact of the system's development and deployment.
- Specific system characteristics that distinguish it from existing or other systems under development.
- Functional, operational, and technical characteristics and parameters integral to the system.

4.6. Program information details the organization and structure of the office responsible for developing and fielding the acquisition system. Use the Program Management Directive as a source document for this information. Use the program description to briefly describe the acquisition chain of

command for the program, including the program's Milestone Authority and any sub-programs, and specify the location, points of contact, and telephone number of the following:

- Government-owned sites that will handle EPITS material.
- Government-owned test and evaluation centers where EPITS material will be tested.
- Primary contractors who handle EPITS materials.
- Contractor-owned facilities where EPITS materials will be tested.

4.7. Base all protection efforts for the program on those EPITS, which give the program or system its unique capability.

4.7.1. A list of EPITS contains those specific items of EPITS that, if known by an adversary, could compromise the combat effectiveness of a weapon system.

4.7.2. Your first step is to identify EPITS, a process in which program managers, engineers, scientists, security professionals, OPSEC managers, and counterintelligence personnel work together to isolate key components. To evaluate the importance of these elements, apply the following question to each. An affirmative answer to any of these questions qualifies an item as an EPITS:

- Could loss of an EPITS result in destruction of the US system?
- Could loss of an EPITS result in degradation of the US system?
- Could loss of an EPITS result in duplication of the US system?
- Could loss of an EPITS require major modifications to maintain the strategic or tactical advantage of the system during its projected operational lifetime?

4.7.3. Prioritize the list of EPITS to emphasize the most important elements during the analysis of the protection costs.

4.7.4. Consider subsystems for possible EPITS. Place special emphasis on any process unique to the system, and identify any activity so unique that it limits the ability of adversaries to copy or counter the system.

**4.8. Threats.** Use all source intelligence to evaluate threats. Air Force Office of Special Investigations (AFOSI) provides adversary threat to Air Force acquisition programs through their Seven Citadels Program.

4.8.1. Program directors, with the AFOSI representative, determine if their particular program requires counterintelligence support. If necessary, provide a threat request to the AFOSI representative. Make the request detailed and specific. Use the list of questions in **Attachment 2** to write the request.

4.8.2. AFOSI analyzes the threat for each program location, the program office site, and each separate test facility. Security costs may vary at different locations.

**4.9. Vulnerabilities.** Vulnerabilities indicate the ways that adversaries collect information. Determine vulnerabilities by comparing the EPITS, with the threat. Use the formula SUSCEPTIBILITY + THREAT = VULNERABILITY. Keep in mind that some systems or products may require a higher level of security than this formula may show. Systems or products that are inherently dangerous to the public or are very expensive or hard to replace must be protected accordingly. Likewise, some systems or products require protection based on higher level directives, such as nuclear weapons.

4.9.1. If a source of information is secure, the information is not SUSCEPTIBLE to collection. If a computer containing EPITS runs as a stand alone in a classified mode, the data is not SUSCEPTIBLE to collection, but a network computer with remote dial up connections is potentially susceptible.

4.9.2. An information source is not a VULNERABILITY unless a collection activity can or is collecting the source. This is the THREAT.

4.9.3. A valid VULNERABILITY requires both a SUSCEPTIBILITY and a THREAT. If either is absent, a VULNERABILITY does not exist.

**4.10. Countermeasures:**

- Develop and propose countermeasures for each identified vulnerability.
- Provide an estimate of required resources (manpower, material, and money) for each proposed countermeasure.
- Make a risk assessment indicating the impact of implementing each countermeasure versus not implementing it and accepting the risk.

4.11. Identify all protection costs for each acquisition phase. Protection costs include manpower, equipment, services and all other costs that contribute to the protection of the program. Coordinate cost estimation with the program control office, as follows:

- Include in manpower costs all personnel who provide direct support to the program protection effort. Your local manpower specialist can guide you in determining manpower cost.
- List equipment used in the protection effort with the associated cost. Include the cost of safes, secure computers, software, entry controls, alarms, construction of vault areas, administrative equipment, and security equipment engineered into the weapon system.
- Identify miscellaneous costs not included in the previous paragraphs. Include temporary duty to support program protection, cost of transporting classified components, security education and training efforts, and contract administrative support. Prepare program protection cost estimates for the current and remaining acquisition phases for programs that have advanced beyond Milestone I. If necessary, use historical cost data as a basis for future estimates.

**5. Time- or Event-Phased Security Classification Guide.** Develop and maintain a time- or event-phased security classification guide for each acquisition program, as follows:

- Prepare the guide after identifying the system's EPITS. The original classification authority must approve the guide no later than the Milestone I.
- Attach the completed guide to the PPP.
- Focus on the EPITS. Consider whether unclassified EPITS should be marked with distribution statements or other protection requirements.

**6. TA/CP.** You must complete a TA/CP and get it approved for all acquisition programs that will have foreign cooperation, co-production, or military sales. Complete a TA/CP before you submit the request for authority to negotiate an international agreement. Coordinate the TA/CP with the appropriate local offices to get approval for foreign disclosure, foreign cooperation or co-production, and foreign military sales (if applicable).

6.1. TA/CP serves three purposes:

- Assesses the feasibility of US participation in joint programs from a foreign disclosure and technical security perspective.
- Drafts the Delegation of Disclosure Authority Letter (DDL). You must have an approved DDL before you can disclose US Air Force information to foreign entities.
- Serves as a supporting document during acquisition decision review.

**6.2. Content.** The TA/CP consists of two sections:

**6.2.1. The Technology Assessment Section.** This section focuses on the risk to the United States of disclosing technology or information to other countries. Identify the technology of concern, its classification or control method, or why it is under development. Evaluate the availability of comparable foreign technology, previously released US technologies, and any material released under other programs. Finally, compare the value in terms of technologies and military capabilities, and possible damage resulting from compromise of these technologies or capabilities.

**6.2.2. The Control Plan Section.** This section describes the measures to minimize potential risk and danger, or susceptibility of compromise associated with the material's release. Discuss phasing the release of information to reduce the risk of compromise, using disclosure restrictions, and using special security procedures to limit access to essential information. Include a discussion of any modification to the system, design, or production produced under the agreement, or any legal or proprietary concerns associated with such an agreement.

6.2.3. The program office prepares a DDL as part of the request for authority to conclude an agreement. SAF/IADP authorizes DDLs, which authorize MAJCOM foreign disclosure offices (FDO) to disclose classified and unclassified US Air Force information to foreign governments and international organizations in accordance with specific conditions, limitations and procedures to support approved international programs.

6.2.4. MAJCOMs can delegate DDL disclosure authority to local or base FDOs with SAF/IADP approval. All disclosures must have appropriate FDO approval. Air Force personnel will not release or imply intent to release documents, information, equipment or technology until a DDL is approved or the disclosure is approved in advance by SAF/IADD. Reference AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations* (formerly AFRs 200-9, 400-10, and 400-43), for further guidance on preparation and coordination of DDLs.

**7. System Security Engineering.** System security engineering applies scientific and engineering principles to identify system vulnerabilities and eliminate or contain risks associated with security vulnerabilities. System security engineering is an essential element of acquisition systems protection and integrates security into the overall systems engineering process.

7.1. System security engineering seeks to eliminate, reduce, or control through engineering and design, any characteristics that could allow deployment of systems with operational security deficiencies. For more detailed information on system security engineering, refer to AFI 31-702.

**8. Program Protection Surveys (PPS).** Conduct at least one protection survey on each ACAT I and ACAT II acquisition program during each phase of the acquisition cycle. Use the PPS to assess the effec-

tiveness of the established program protection following PPP approval and implementation. Use the guide in **Attachment 2** to plan and conduct a program protection survey.

8.1. The PPS meets the survey requirements of DoD Instuction 5000.2 by simulating an intelligence collection effort aimed at the critical information of a specific acquisition program at a specific center, Research, Development, Testing, and Evaluation laboratory, or test facility. The PPS is the program director's primary tool to evaluate and validate the current protection plan.

8.2. PPS objectives are to:

- Assess the overall effectiveness of the PPP during a given phase of the acquisition process.
- Provide specific indicators of possible losses of protected elements.
- Provide specific information on how the loss of protected elements occurred.
- Provide information to update the PPP for the remaining acquisition phases.

8.3. The survey provides the program director with information about the effectiveness of the security applied to the program. Based on this information, the program director may continue the PPP as written, or refocus the security resources to eliminate any security short falls.

8.3.1. Use simulated collection with minimal manpower, in a limited time frame to identify, reduce, or eliminate exploitable vulnerabilities to the acquisition program. Determine if the previously identified EPITS received adequate protection during a given phase of the acquisition process. Focus on specific, valid threat and countermeasures.

8.3.2. Limit the survey to determine the effectiveness of the protection and countermeasures planned and implemented at a specific facility to protect the EPITS of a selected acquisition program.

8.3.3. Provide a written report on:

- The adversary intelligence collection threat.
- Effectiveness of the protection measures applied to the program EPITS.
- Recommendations to improve protection measures to eliminate or reduce identified vulnerabilities.

8.3.4. Provide this report to the program director and the program security manager.

8.3.5. In addition, provide a "lessons learned" report discussing the specific area of PPP strengths and weaknesses. This must be an abbreviated report. Omit actual locations, personal names and other program identifying information. Use this report to identify common problems in the acquisition community.

8.3.6. Identify generic problems with resources, facilities, or training of the acquisition community. Forward the lessons learned report through appropriate channels to the command OPSEC office.

8.3.7. Do not conduct a PPS at contractor-owned or operated locations unless the provisions of the contract authorize compliance inspections. Coordinate surveys with the local Defense Investigative Service office.

8.3.8. Use other available security surveys where possible to avoid the cost of a PPS.

8.3.9. Conduct the PPS at the most vulnerable and riskiest locations. Do not conduct a PPS at a location where low risk exists and where EPITS are not especially vulnerable.

**9. Additional Security Plans.** Attach additional security plans required by the SSWG as tabs to the PPP, for example:

- TEMPEST Plan.
- Computer Systems Security Accreditation Plan.
- Sensitive Compartmented Information Facility Accreditation Plan.
- System Security Management Plan.
- Weapon System Security Standard.

**10. PPP Review Process:**

10.1. The program manager coordinates the PPP with the MAJCOM(s) that own or operate the system. After coordination, the program manager forwards the PPP to the Air Force Acquisition Executive for approval. For ACAT ID, ACAT IC and II, programs, forward the PPP to SAF/AQX. For ACAT III and IV programs forward the PPP to the Designated Acquisition Commander for approval.

10.2. All affected security disciplines participate in a coordinated review of the PPP. For ACAT I and II programs, SAF/AQX coordinates the review of the PPP among the responsible security policy offices and makes updates or corrections. SAF/AQX then forwards the PPP to the Air Force Acquisition Executive for approval of ACAT IC and II programs, and to the Acquisition Systems Protection Office for review of ACAT ID programs.

10.3. Update the PPP using the same review process before each Milestone, or when significant changes occur to EPITS, threat, or the physical environment.

**11. Acronyms Used:**

**ACAT—**Acquisition Category

**AFOSI—**Air Force Office of SpecialInvestigations

**DDL—**Disclosure Authority Letter

**DoD—**Department of Defense

**EPITS—**Essential Program Information,Technologies, and Systems

**FDO—**Foreign Disclosure Office

**MAJCOM—**Major Command

**OPSEC—**Operations Security

**PPP—**Program Protective Plan

**PPS—**Program Protection Surveys

**SPO—**System Program Office

**SSWG—**System Security WorkingGroup

**TA/CP—**Technology Assessment/Control Plan

STEPHEN C. MANNELL, Brig General, USAF
Chief of Security Police

## Attachment 1

## PROGRAM PROTECTION PLAN KEY EXIT CRITERIA

**A1.1.** Does the summary of the system description identify the system's mission, military value, and expected operational parameters?

**A1.2.** Does the description of the EPITS identify the significant technical parameters, which, if compromised, would reduce the combat effectiveness or combat effective lifetime of the system?

**A1.3.** Does the threat and or vulnerability analysis:

- Identify who has the interest and capability to collect information about the system?
- Indicate which other countries are performing research in these areas, what is the level of sophistication, and how well they are protecting or controlling the information?

**A1.4.** Does the countermeasures program:

- Indicate that it is time or event driven in its implementation or termination of protection strategies?
- Commit to a level of protection or security concept that will assure a minimal level of protection for the essential elements?

**A1.5.** Does the cost criteria provide the data by acquisition phase?

## Attachment 2

## INFORMATION AND QUESTIONS TO CONSIDER WHEN REQUESTING A THREAT ASSESSMENT

Classify as directed by an Original Classification Authority or derivatively.

**A2.1.** Name of Program/Project/Product.

**A2.2.** Program/Project/Product Manager, Organization, Location, and Telephone Numbers.

**A2.3.** Security Manager Address and Telephone Numbers.

**A2.4.** Contract Numbers/Prime Contractor/Location/Mailing Address/Security Manager/Telephone number.

**A2.5.** Major Subcontractors/Address/Subcontract numbers/Security Managers/Telephone Numbers.

**A2.6.** Against what will the system be targeted?

**A2.7.** What are the program's EPITS?

**A2.8.** What specific technologies do you need to protect. Which contractors are involved?

**A2.9.** What specific information of core technologies is classified? Is special access program technology involved?

**A2.10.** Where are the technologies located? (Answers can include aboard aircraft, within buildings, mounted in vehicles, man-packed, and so on.)

**A2.11.** If the material is a weapons system, what specific component or components require protection? (For example, answers can include possible sights, range finder, target acquisition system, and so on. Also state whether the system or technology is touch or sight sensitive.)

**A2.12.** If you are protecting a computer system, what specific component of the system requires protection? (Answers can include software, hardware, and so on.)

- Is the system stand alone or networked?
- Can you access the system from other systems at other facilities or bases?
- Are links between systems encrypted?
- How are the systems linked? (Answers can include dedicated land lines, microwave, and so on.)

**A2.13.** If an aircraft is involved, what specific component of the aircraft requires protection? (Answer can include items such as electronic system, weapon system, crew, and so on.)

- Can you remove the components from the aircraft?
- Can you see the components from outside the aircraft?

**A2.14.** If vehicles are involved, are the vehicles dedicated to this system or activity?

- Are these vehicles unique to this system or activity?
- Can you see the system components from outside the vehicle?
- Can you remove the components of the system from the vehicle?

**A2.15.** What are the identifiable, exploitable characteristics of the technology?

- Are there unique physical characteristics involved?
- Can you see the characteristics of the system from outside it?
- Does the system have an electronic signal emission?
- What is the system's operating frequency range?
- Is the system active or passive?
- What is the system's power output?
- What is the system's range?

**A2.16.** Are there specific communications associated with this system?

- Where are these systems employed? (Indicate the location of bases or facilities.)
- Where are these systems employed? (Indicate the location of bases, or facilities.)
- How will you use the system?

**A2.17.** With what facilities is the system associated?

- Are the facilities unique to the system?
- Can you see the facilities from the outside?
- Where are the facilities located? (Specify the location, such as military base, civilian community, industrial complex, public building, and so on.)
- What access controls exist for the building?

**A2.18.** What aspects of the training must you protect? (Indicate particular activities, participants, location, association with system, and so on.)

**A2.19.** Where will you do the system testing? (Indicate any previous test dates, locations, as well as future test dates and locations.)

**A2.20.** Is the system site sensitive (that is, are you worried about the site being seen)? If yes, why?

**A2.21.** What types of emissions to systems tests or test sensors generate?

**A2.22.** Has or will any testing be done against actual or simulated foreign equipment? If yes, identify the foreign equipment, test locations, and dates.

**A2.23.** Do any plans exist, or have there been inquiries about, foreign involvement (for example, foreign sales, foreign cooperative development, co-production, joint ventures, and so on)? If yes, with whom are negotiations taking place what is and the current status?

**A2.24.** What are the major milestone dates for this program?